PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-291740
(43)Date of publication of application : 03.12.1990

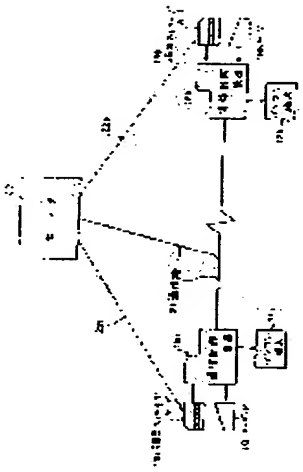
(51)Int.Cl. H04L 9/32

(21)Application number : 01-109169
(22)Date of filing : 01.05.1989

(71)Applicant : FUJITSU LTD
(72)Inventor : AKIYAMA RYOTA
TORII NAOYA

(54) KEY DELIVERY SYSTEM WITH SIGNATURE FUNCTION

(57)Abstract:
PURPOSE: To disable a person, who steals key information to try the access to a terminal but does not know secret information, to decode a cipher by combining discrimination information and secret information at the time of generating a common key.
CONSTITUTION: A center 20 generates two parameters Zi and kk for a user (i) and writes them on a magnetic stripe card 19 corresponding to the user (i) and delivers this card to the user (i). Similar parameters whose subscript is changed to (k) are generated for a user (k) to deliver the card to a user (k). Users (i) and (k) read delivered magnetic stripe cards 19 from a card reader 26 and manage them as a user management file. The parameter Zk which the user (i) receives from the user (k) of the other party includes the reciprocal of an open parameter IDk and a password pwk of the terminal of the other party; and when the user (i) generates the common key, he is requested to input not only IDk of the user (k) of the other party but also a password pwi of the user (i) from a keyboard.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平2−291740

⑤1Int. Cl.⁵　識別記号　庁内整理番号　⑬公開　平成2年(1990)12月3日
H 04 L 9/32
6945−5K　H 04 L 9/00　A

審査請求　未請求　請求項の数 5　（全9頁）

⑤4発明の名称　署名機能を持つ鍵配送方式

⑳特　願　平1−109169
㉒出　願　平1(1989)5月1日

⑦2発明者　秋山　良太　神奈川県川崎市中原区上小田中1015番地　富士通株式会社内
⑦2発明者　鳥居　直哉　神奈川県川崎市中原区上小田中1015番地　富士通株式会社内
⑦1出願人　富士通株式会社　神奈川県川崎市中原区上小田中1015番地
⑦4代理人　弁理士　大菅　義之　外1名

明　細　書

1．発明の名称

署名機能を持つ鍵配送方式

2．特許請求の範囲

1）通信を行う2つの端末の暗号化鍵と復号鍵を相互に等しい共通鍵とし、前記各端末間で通信文を前記共通鍵により暗号化して暗号文として送信し、受信した該暗号文を前記共通鍵により復号して通信文として受信する共通鍵暗号化方式において、

複数の端末(1)の各々に、

自己端末の識別情報及び自己端末の秘密情報を構成要素として含む鍵情報(3)を予め保持し、暗号文(10)の通信開始前に相手端末に転送する鍵情報制御手段(2)と、

暗号文(10)の通信開始前に相手端末の識別情報(5)と自己端末の秘密情報(6)を入力させる入力手段と、

暗号文(10)の通信開始前に前記相手端末から転送されてくる前記鍵情報(3)を前記入力手段(4)から入力された前記相手端末の識別情報(5)及び前記自己端末の秘密情報(6)を含む情報に基づいて変換して共通鍵(8)を生成する共通鍵生成手段(7)とを有することを特徴とする署名機能を持つ鍵配送方式。

2）前記識別情報はＩＤデータであり、

前記自己端末の秘密情報は自己端末のパスワードデータであり、

前記鍵情報は、所定の整数をベキ乗して得られるデータ値であり、該ベキ乗の項には前記自己端末のＩＤデータの逆数と前記自己端末のパスワードデータとの積の項が含まれ、

前記共通鍵生成手段は、前記相手端末から送られてくる前記鍵情報であるデータ値をベキ乗して前記共通鍵を生成し、該ベキ乗の項には前記入力手段から入力された前記相手端末のＩＤデータと前記自己端末のパスワードデータとの積の項が含まれることを特徴とする請求項1記載の署名機能

を持つ鍵配送方式。

3）前記識別情報はＩＤデータであり、

前記自己端末の秘密情報は自己端末のパスワードデータであり、

前記鍵情報は、所定の整数をベキ乗して得られる値について所定の合成数に対する剰余を演算して得られるデータ値であり、該ベキ乗の項には前記自己端末のＩＤデータの逆数と前記自己端末のパスワードデータとの積の項が含まれ、

前記共通鍵生成手段は、前記相手端末から送られてくる前記鍵情報であるデータ値をベキ乗して得られる値について前記所定の合成数に対する剰余を演算することにより前記共通鍵を生成し、該ベキ乗の項には前記入力手段から入力された前記相手端末のＩＤデータと前記自己端末のパスワードデータとの積の項が含まれることを特徴とする請求項１記載の署名機能を持つ鍵配送方式。

4）前記各端末を統括管理するセンタ管理部を有し、

該センタ管理部は、前記各端末に該各端末毎の前記鍵情報を予め供給することを特徴とする請求項１、２又は３記載の署名機能を持つ鍵配送方式。

5）前記共通鍵生成手段において演算される前記ベキ乗の項には、更に通信文番号データと日付データとの積の項が含まれることを特徴とする請求項２、３又は４記載の署名機能を持つ鍵配送方式。

3．発明の詳細な説明

〔概　　要〕

通信を行う２つの端末の暗号化鍵と復号鍵を相互に等しい共通鍵とし、各端末間で通信文と暗号文との間で共通鍵により暗号化／復号を行う共通鍵暗号化方式に係り、更に詳しくは、通信開始前に相互に鍵情報を交換しあって各端末で共通鍵を生成する場合の署名機能を持つ鍵配送方式に関し、

任意の相手端末との間で各端末の認証が可能なユニークな署名付の共通鍵を実現し、共通鍵の生成過程が簡単で、かつ、各端末毎の秘密パラメータを、磁気ストライプカードのようにガードの比較的緩いもの等で安全かつ容易に管理できるようにすることを目的とし、

複数の端末の各々に、自己端末の識別情報及び自己端末の秘密情報を構成要素として含む鍵情報を予め保持し、暗号文の通信開始前に相手端末に転送する鍵情報制御手段と、暗号文の通信開始前に相手端末の識別情報と自己端末の秘密情報を入力させる入力手段と、暗号文の通信開始前に前記相手端末から転送されてくる前記鍵情報を前記入力手段から入力された前記相手端末の識別情報及び前記自己端末の秘密情報を含む情報に基づいて変換して共通鍵を生成する共通鍵生成手段とを有するように構成する。

〔産業上の利用分野〕

本発明は、通信を行う２つの端末の暗号化鍵と復号鍵を相互に等しい共通鍵とし、各端末間で通信文と暗号文との間で共通鍵により暗号化／復号を行う共通鍵暗号化方式に係り、更に詳しくは、通信開始前に相互に鍵情報を交換しあって各端末で共通鍵を生成する場合の署名機能を持つ鍵配送方式に関する。

〔従来の技術〕

近年、企業内通信網の普及は著しく拡大している。しかし、企業内通信において、人事情報，社内機密情報，資金情報等重要なデータを通信網を使って送る場合、第３者による通信盗聴・傍受・通信当事者による誤配送等の問題があり、暗号化技術が重要視されている。

暗号化技術において、通信を行う２つの端末の暗号化鍵と復号鍵を相互に等しい共通鍵とし、各端末間で通信文と暗号文との間で共通鍵により暗号化／復号を行う共通鍵暗号化方式がある。そして、共通鍵を生成する方式として、通信開始前に相互に鍵情報を交換しあって各端末で共通鍵を生成する方式がある。

上記暗号化技術においては、共通鍵を生成するための鍵情報（以下、単に鍵と呼ぶ）を各端末で管理する必要があるが、通信網への加入者数が数千ないし数万と数が増大すると、鍵管理が複雑化

し管理すべき鍵が膨大なものとなって、通信の安全性が保てなくなる。

鍵管理の従来方式として、ＩＤ番号（各端末の識別番号）を利用した鍵管理方式がある。これは、通信を行う各端末のＩＤ番号を共通鍵の生成情報として用いる方式である。

〔発明が解決しようとする課題〕

しかし、上記従来例の場合、生成された共通鍵には、通信当事者間の各個人が管理する暗証番号、パスワード等の秘密情報がからめてなく、通信後に通信当事者間で電文の送受信をめぐるトラブルが生じた場合、正当な調停者は電文送受の事実を立証するのが困難であり、また、共通鍵の生成過程が複雑で、各ユーザの管理する秘密パラメータをＩＣカード等のガードの強固なもので管理する必要がある等の問題点を有している。

本発明は、任意の相手端末との間で各端末の認証が可能なユニークな署名付の共通鍵を実現し、共通鍵の生成過程が簡単で、かつ、各端末毎の秘密パラメータを、磁気ストライプカードのようにガードの比較的緩いもの等で安全かつ容易に管理できるようにすることを目的とする。

〔課題を解決するための手段〕

第１図は、本発明のブロック図である。本発明は、通信を行う２つの端末の暗号化鍵と復号鍵を相互に等しい共通鍵とし、各端末間で通信文を共通鍵により暗号化して暗号文として送信し、受信した該暗号文を共通鍵により復号して通信文として受信する共通鍵暗号化方式を前提とする。

本発明は、複数の端末1_1、1_k・・・の各々に、以下の鍵情報制御手段、入力手段及び共通鍵生成手段を有する。

鍵情報制御手段2_1、2_k・・・は、自己端末の識別情報及び自己端末の秘密情報を構成要素として含む鍵情報3_1、3_k・・・を予め保持し、暗号文の通信開始前に相手端末1_1又は1_kに、例えば通信路１１を介して転送する手段である。ここで、上記識別情報は例えばＩＤデータであり、自己端末の秘密情報は例えば自己端末のパスワードデータである。そして、鍵情報3_1、3_k・・・は、例えば所定の整数をベキ乗して得られるデータ値であり、該ベキ乗の項には自己端末のＩＤデータの逆数と自己端末のパスワードデータとの積の項が含まれる。又は、鍵情報3_1、3_k・・・は、例えば上記ベキ乗して得られた値について所定の合成数に対する剰余を演算して得られるデータ値としてもよい。

入力手段4_1、4_k・・・は、暗号文の通信開始前に相手端末の識別情報5_k、5_1・・・と自己端末の秘密情報6_1、6_k・・・を入力させる手段である。相手端末の識別情報5_1、5_k・・・は、前述のように例えばＩＤデータであり、自己端末の秘密情報6_1、6_k・・・は、前述のように例えば自己端末のパスワードである。

共通鍵生成手段7_1、7_k・・・は、暗号文の通信開始前に、相手端末1_k、1_1・・・から例えば通信路１１を介して転送されてくる鍵情報3_k、3_1・・・を、入力手段4_1、4_k・・・から入力された相手端末の識別情報5_k、5_1・・・と自己端末の秘密情報6_1、6_k・・・を含む情報に基づいて変換して共通鍵８を生成する手段である。同手段は、例えば相手端末1_k、1_1・・・から送られてくる鍵情報であるデータ値3_k、3_1・・・をベキ乗して共通鍵８を生成し、該ベキ乗の項には入力手段4_1、4_kから入力された相手端末1_k、1_1・・・のＩＤデータ5_k、5_1・・・と自己端末のパスワードデータ6_1、6_k・・・との積の項が含まれる。又は、上記ベキ乗して得られる値について前記所定の合成数に対する剰余を演算することにより共通鍵８を生成するようにしてもよい。また、上記ベキ乗の項には、更に通信文番号データと日付データとの積の項が含まれるようにしてもよい。　上記のようにして生成される共通鍵８を用いることにより、各端末1_1、1_kにおいて、同図12_1、12_kのように、通信文9_1と10_1又は9_kと10_kの間で暗号化又は復号が行われる。

一方、本発明で、上記各構成に加えて、各端末

1_i、1_k・・・を統括管理するセンタ管理部13を有する構成にできる。同管理部は、各端末1_i、1_k・・・に該各端末毎の鍵情報2_i、2_k・・・を、予め例えば磁気ストライプカードの形態で供給する。

〔作　　用〕

自己の端末例えば1_iが相手の端末例えば1_kの鍵情報制御手段2_iから鍵情報3_kを受け取る場合、同鍵情報3_kには相手端末1_kの識別情報と相手端末1_kの秘密情報が含まれている。そして、自己端末1_iの共通鍵生成手段7_iで共通鍵8を生成する場合、入力手段4_iから、相手端末の識別情報5_kのほかに自己端末の秘密情報6_iを入力することも要求される。従って、端末1_iの鍵情報3_iを他人が盗み、端末1_iを操作して端末1_kをアクセスしようとしても、その他人は自己端末の秘密情報6_i（パスワード等）がわからなければ、相手端末1_k側で生成される共通鍵8と同じ共通鍵8を生成することができないため、暗号化又は復号を行えず、非常に安全性の高い暗号通信を実現できる。

この場合、共通鍵生成手段7_iにおいて、例えば所定の整数のベキ乗又は更に剰余を演算するだけで、共通鍵8を生成できるため、共通鍵の作成過程が簡単になる。

また、各端末毎1_i、1_k・・・の鍵情報3_i、3_k・・・は、例えばセンタ管理部13から第1図の破線14_i、14_k・・・のように供給されるが、この場合、各鍵情報3_i、3_k・・・が盗まれただけでは前述のように暗号を解読できないため、上記供給は例えば磁気ストライプカードのようにガードの比較的緩いもので行える。

一方、各共通鍵生成手段7_i、7_kで共通鍵8を生成する場合、前記ベキ乗の項に通信文データと日付データの積の項を含ませることにより、例えば後にトラブルが発生した場合、センタ管理部13は共通鍵8の内容を確認することにより、電文（通信文）送受の事実の立証を容易に行うことができる。

〔実　施　例〕

以下、図面を参照しながら本発明の実施例の動作を説明する。

第2図は、本実施例の全体システム構成図である。

同図において、まず、各パソコン端末17_i、17_kを操作して通信を行うユーザi、kは、センタ20より支給される磁気ストライプカード19_i、19_kを、各通信制御装置16_i、16_kへセットする。

その後、各ユーザi、kは、通信開始前に各キーボード18_i、18_kから後述する必要なパラメータを入力しする。そして、パソコン端末17_iと17_kの間で、通信制御装置16_i、16_k及び通信路21を介して、暗号通信を行う。

なお、第2図の実施例では、通信制御装置16_i及び16_k等は、ユーザiとkの2人分に対応する分のみ示してあるが、当然多数の装置が通信路21を介して接続されている。

第3図は、第2図の通信制御装置16_i、16_kの構成図である。同図で、通信制御装置16は、第2図の16_i及び16_kに対応し、キーボード18は第2図の18_i及び18_kに対応し、磁気ストライプカード19は、第2図の19_i及び19_kに対応する。

カードリーダ23は、第2図のセンタ20から供給される磁気ストライプカード19の内容を読み取り、後述する必要なパラメータをベキ乗剰余演算器24に入力させる。

上記磁気ストライプカード19の内容は、ベキ乗剰余演算器24で自己のユーザIDが付加され、そのまま送受信装置26へ送られる。

一方、相手側通信者も同様な構成の装置を持ち、相手側も相手の固有のIDと上記データを送りかえし、そのデータは送受信装置26で受信されベキ乗剰余演算器24へ入力される。

これと共に、キーボード18より入力される自己のIDとパスワードがベキ乗剰余演算器24へ入力し、後述するベキ乗剰余演算処理が行われる。

この結果得られた後述する共通鍵は、共通鍵保

管装置２５へ記憶されると共に、同装置を介して暗号装置２７の鍵入力へセットされる。

暗号装置２７は、パソコン１７側の平文データと通信路２１側の暗号文との間で暗号化又は復号を行う。

一方、通信を申し込まれた相手側は、通信終了後、共通鍵保管装置２５に保管された共通鍵にその時の日付を付して、暗号装置２７、送受信装置２６及び通信路２１を介して第２図のセンタ２０へ送る。

以下、上記第２図及び第３図の構成の実施例の動作を、第４図の動作説明図に沿って説明する。なお、特に言及しない限り第２図及び第４図を随時参照するものとする。

まず、センタ２０内には、特には図示しない例えばディスク記憶装置内等に、第４図に示されるセンタ管理ファイル２８を記憶している。同ファイルとしては、秘密のパラメータｃ、ｎ＝ｐ×ｑ（ｐ、ｑは素数）、ｅ，ｄ、但しｅ・ｄ＝１ mod｛ＬＣＭ（ｐ－１)(ｑ－１）｝、各ユーザが予め登録した秘密パラメータ（パスワード：pw_1，pw_2，・・・，pw_n）、及び各ユーザの識別番号である公開パラメータ（ID_1，ID_2，・・・，ID_n）を管理する。ここで、ＬＣＭは最小公倍数をあらわす。ここで、ＬＣＭは最小公倍数を表す。

そして、センタ２０は、まず、２つのパラメータ $Z_i = M^{e \cdot (ID_i)^{-1} \cdot pw_i}$（ここで ID_i^{-1} は $ID_i^{-1} \times ID_i \equiv 1 \bmod \{LCM((p-1)(q-1))\}$ の関係を使って求める）、及び $kk = c \cdot e$ をユーザｉのために作成し、これらをユーザｉに対応した磁気ストライプカード１９に書き込み、ユーザｉへ配る。なお実際には、Z_i の剰余が計算されるが、以下の説明では簡単のため、まず、剰余を演算しないものとして説明し、そのあとで剰余を演算する意味及び演算方法について説明する。ここで、演算「＊」は乗算を意味する。

センタ２０は、ユーザｋに対しても添え字がｋになった同様のパラメータを作成・配給する。他の特には図示しない複数のユーザに対しても同様の操作が行われる。

各ユーザｉ、ｋは、配られた磁気ストライプカード１９をカードリーダ２３から読み込み、第４図のユーザ管理ファイル29_i、29_kとして管理する。なお、このファイルは、例えばベキ乗剰余演算器２４内の特には図示しない記憶装置等に一時記憶される。

ユーザｉがユーザｋと通信を開始したい場合、ユーザｉはベキ乗剰余演算器２４から送受信装置２６を介して、ユーザｋの通信制御装置16_kへ上記パラメータZ_iを転送する。同様に、ユーザｋもユーザｉの通信制御装置16_iに対し、パラメータZ_kを転送する。

ユーザｉは、ベキ乗剰余演算器２４において、ユーザｋから送受信装置２６を介して受信されたパラメータZ_kに対し、ユーザｉがセンタ２０からもらったパラメータｋｋ、及び予めキーボード１８から入力した自己のパスワードpw_iとユーザｋのID_k（ユーザｋの名前，住所，電話番号等ｋ本人を示す公的な情報）等を使って、第４図に示すように、$Z_k^{kk \cdot ID_k \cdot pw_i}$ なる演算を行う。この演算の結果、第４図の29_kとの関係より、$M^{e \cdot pw_i \cdot pw_k}$ なる共通鍵が得られる。なお、実際にはこの値に対しても剰余が演算されるがこれについては後述する。上記共通鍵は共通鍵保管装置２５に記憶される。

一方、ユーザｋ側も上記ユーザｉと同様な操作が行われる。即ち、ベキ乗剰余演算器２４において、受信したパラメータZ_iに対し、ユーザｋがセンタ２０からもらったパラメータｋｋ、及び予めキーボード１８から入力した自己のパスワードpw_kとユーザｉのID_i（ｉの名前，住所，電話番号等ｉ本人を示す公的な情報）等を使って、$Z_i^{kk \cdot ID_i \cdot pw_k}$ なる演算を行う。この演算の結果、ユーザｉ側と全く同じ$M^{e \cdot pw_i \cdot pw_k}$ なる共通鍵が得られる。この共通鍵は共通鍵保管装置２５に記憶される。

以上の操作の後、共通鍵保管装置２５の共通鍵が暗号装置２７に入力し、親展通信を実現する暗号装置の鍵として利用される。

通信終了後、ユーザkは共通鍵に日付を付し、これらの情報を例えば暗号装置２７から送受信装置２６及び通信路２１を介してセンタ２０に通知する。

以上の操作において、センタ２０から各ユーザiとkに提供されるパラメータZ_iとZ_k等、及び各ユーザiとkのベキ乗剰余演算器２４で演算される共通鍵$M^{c \cdot PWi \cdot PWk}$は、実際にはそれらの剰余が演算されて使用される。これは、単純にベキ乗を演算するとパラメータの値がオーバーフローする可能性があること、剰余をとることによりパスワード等の秘密保持性を高められること等の理由による。これらの剰余演算は、以下のようにして実現される。

センタ２０におけるZ_i（Z_kに対してもiとkが異なるのみで同様である）の合成数nに対する剰余演算$Z_i \pmod n$は、まず、$M^d \pmod n$が演算され、次に、その値が$(ID_i)^{-1}$乗された後、再びmod nが演算され、最後にその値がpw_i乗される。これにより、$Z_i = M^{d \cdot (IDi)^{-1} \cdot PWi}$に対する剰余mod nが演算される。

ユーザiにおける$Z_k^{kk \cdot IDk \cdot PWi}$の合成数nに対する剰余演算$Z_k^{kk \cdot IDk \cdot PWi} \pmod n$は、まず、$Z_k^{kk} \pmod n$が演算され、次に、その値が$ID_k$乗された後、再びmod nが演算されて、その値が$pw_i$乗される。これにより、$Z_k^{kk \cdot IDk \cdot PWi}$の剰余mod nが演算される。

以上に示したように、ユーザiが相手のユーザkから受け取るパラメータZ_kには、第４図２９$_k$に示されるように、相手端末の公開パラメータID_kの逆数とパスワードpw_kが含まれている。そして、ユーザiが共通鍵を生成する場合、キーボード１８から、相手のユーザkのID_kのほかにユーザiのパスワードpw_iを入力することを要求される。従って、例えばユーザiの磁気ストライプカード１９を他人が盗み、ユーザkをアクセスしようとしても、その他人はユーザiのパスワードpw_iがわからなければ、相手のユーザk側で生成される共通鍵$M^{c \cdot PWi \cdot PWk}$と同じ共通鍵を生成することができないため、暗号の解読を行うことができない。従って、非常に安全性の高い暗号通信が実現できる。

また、上記のようにZ_i、Z_k等の内容が盗まれただけでは暗号を解読できないため、センタ２０から各ユーザへの上記パラメータの供給は、磁気ストライプカード１９のようなガードの緩い媒体手段でよいことになる。

更に、例えば後にトラブルが発生した場合、センタ２０は各ユーザから通信終了後に通知されていた共通鍵の内容を解析することにより、どのユーザ間で通信が行われたかという事実を容易に立証できる。

次に、第５図は、第２図及び第３図の構成を基本とする本発明の他の実施例の動作説明図である。

第４図と異なる点は、ユーザiが相手から送られてきたパラメータZ_kから共通鍵を生成する場合、同図の$Z_k^{kk \cdot IDk \cdot PWi \cdot N \cdot T}$として示されるように、通信を行う文書番号N及び日付Tの情報をベキ乗の項にからめている点である。

このようにすることにより、例えば後にトラブルが発生し、センタ２０が各ユーザから通信終了後に通知される共通鍵を解析する場合、アクセスされた文書やその日付の情報まで解析することが可能となる。

〔発明の効果〕

本発明によれば、共通鍵を生成する場合、識別情報と秘密情報をからませたことにより、鍵情報を他人が盗み、ある端末をアクセスしようとしても、秘密情報がわからなければ暗号の解読を行えないようにすることができるため、非常に安全性の高い暗号通信を実現できる。

この場合、共通鍵は、例えば所定の整数のベキ乗又は更に剰余を演算するだけで生成できるため、共通鍵の作成過程が簡単になる。

また、各端末に鍵情報を供給する場合、上述ように鍵情報が盗まれただけでは暗号を解読できないため、その供給は例えば磁気ストライプカードのようにガードの比較的緩いもので行え、供給コストを非常に安価にすることが可能となる。

加えて、各共通鍵生成手段で共通鍵を生成する

場合、ベキ乗の項に通信文データと日付データの積の項を含ませることにより、例えば後にトラブルが発生した場合、センタ管理部は共通鍵の内容を確認することにより、電文（通信文）送受の事実の立証を容易に行うことが可能となる。

4．図面の簡単な説明

第1図は、本発明のブロック図、

第2図は、本実施例の全体システム構成図、

第3図は、本実施例による通信制御装置の構成図、

第4図は、本実施例の動作説明図、

第5図は、他の実施例の動作説明図である。

1i、1k・・・端末、

2i、2k・・・鍵情報制御手段、

3i、3k・・・鍵情報、

4i、4k・・・入力手段、

5i、5k・・・相手端末の識別情報、

6i、6k・・・自己端末の秘密情報、

7i、7k・・・共通鍵生成手段、

8・・・共通鍵、

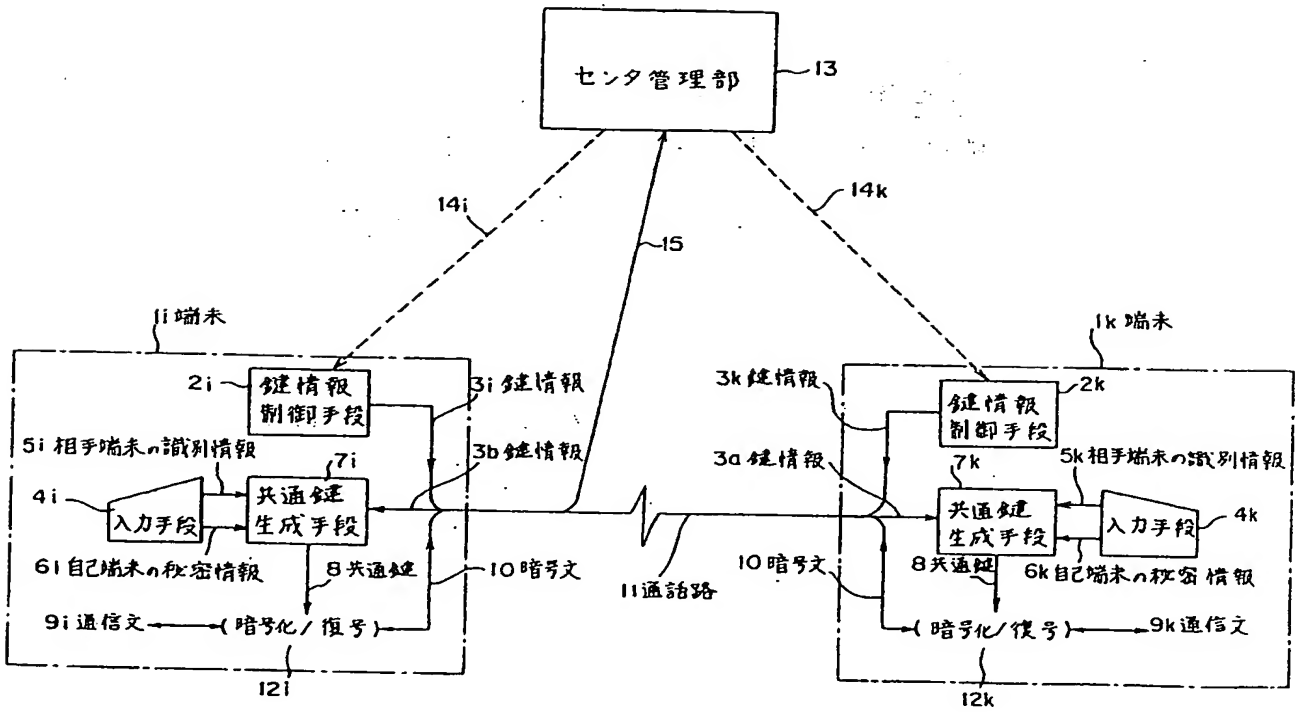
9i、9k・・・通信文、

10・・・暗号文、

11・・・通信路、

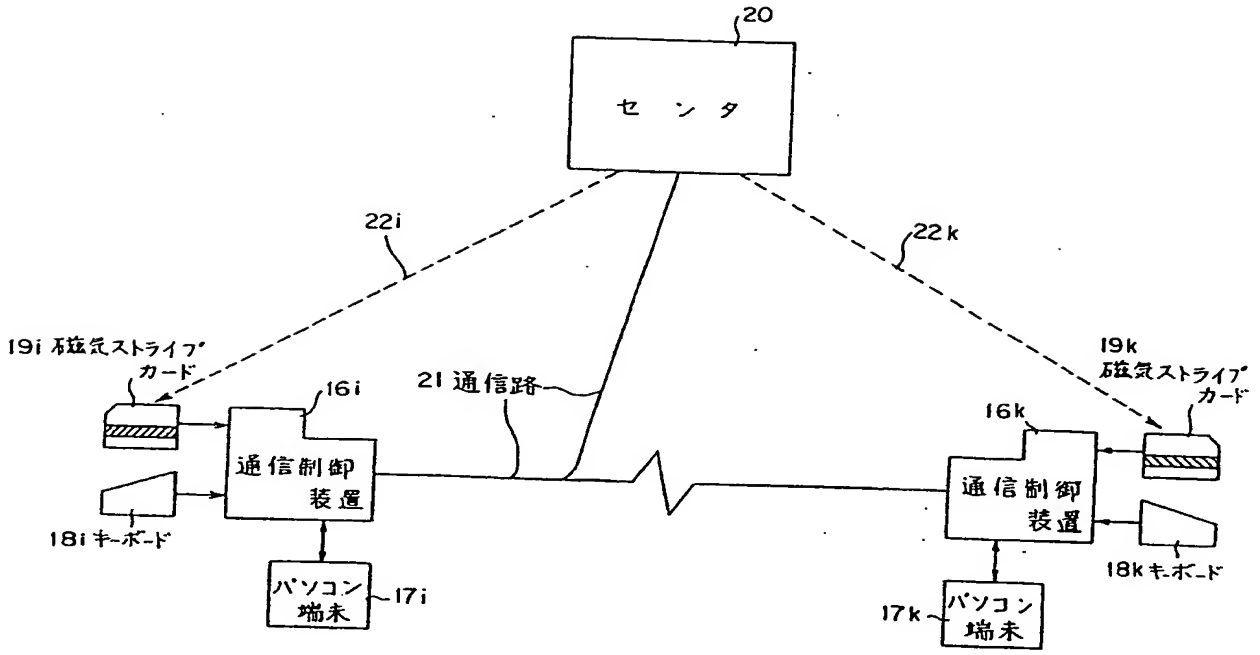
13・・・センタ管理部.

特許出願人　　富士通株式会社



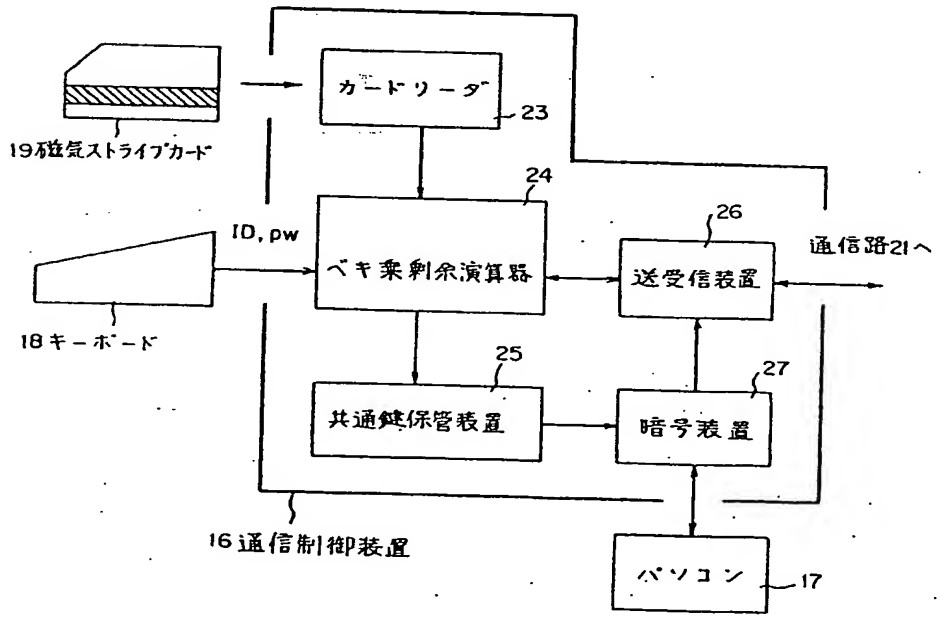
本発明のブロック図

第1図



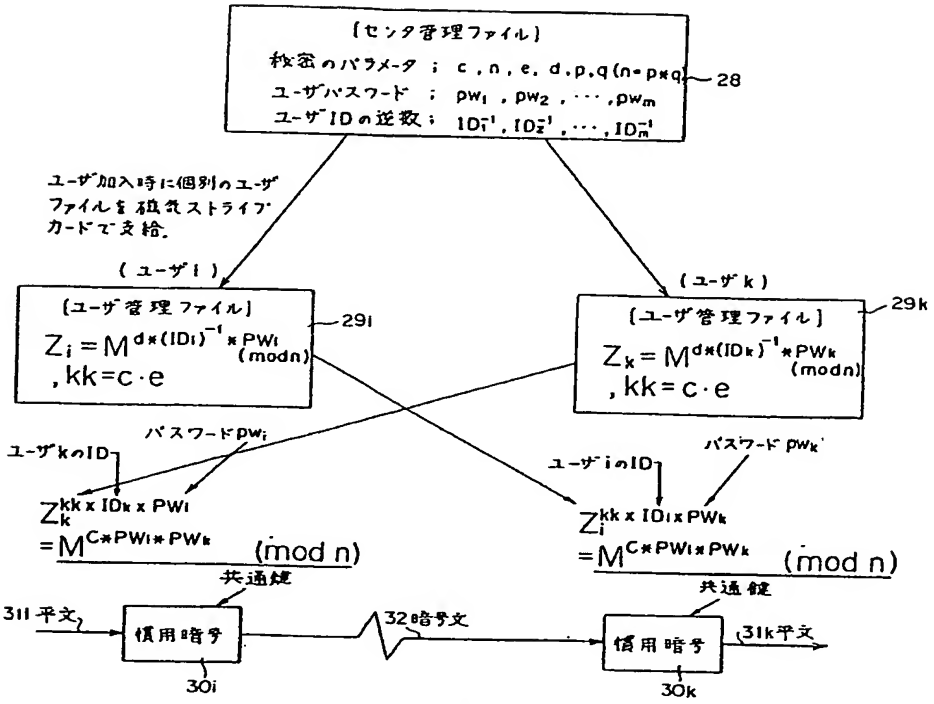
本実施例の全体システム構成図

第 2 図

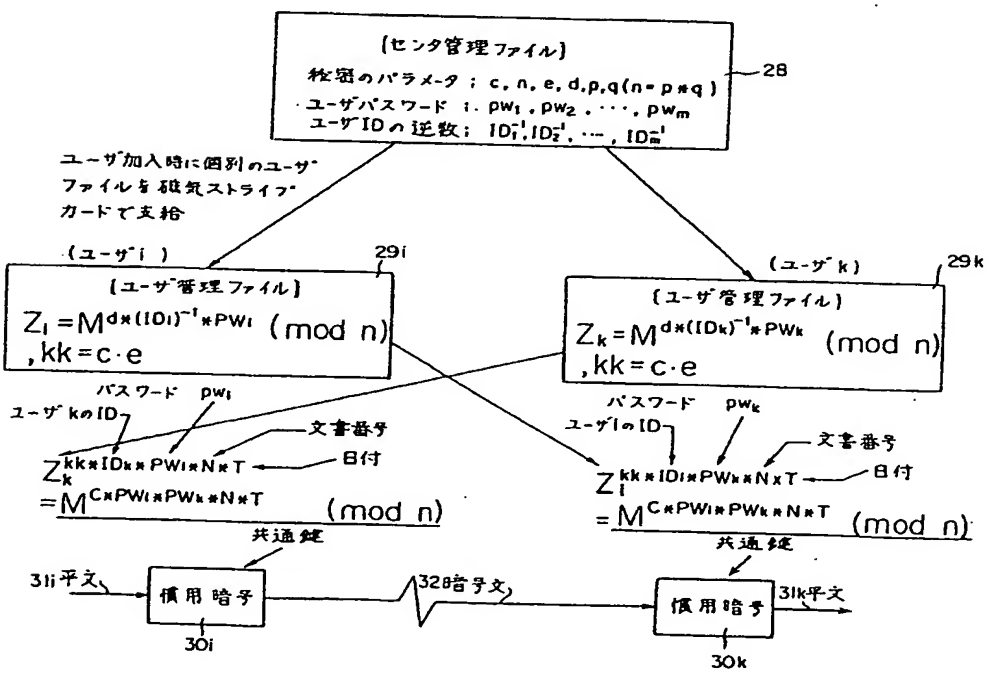


本実施例による通信制御装置の構成図

第 3 図



本実施例の動作説明図
第 4 図



他の実施例の動作説明図
第 5 図